NOT MEASUREMENT SENSITIVE

MIL-STD-2045-18500-1
28 October 1993

MILITARY STANDARD

Information Technology
DoD Standardized Profiles AMHXn(D)
Message Handling Systems
Message Security Protocol
(MSP)

Part 1: MSP Service Support

AMSC N/A **AREA DCPS**

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

Foreword

This military standard is approved for use by all Departments and Agencies of the Department of Defense (DoD).

Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this MIL-STD should be addressed to the:

Joint Interoperability and Engineering Organization (JIEO)
ATTN: TBBD
Building 286
Fort Monmouth, New Jersey 07703-5613

by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this MIL-STD or by memorandum.

This DoD Standardized Profile (DSP) is a functional standard produced by the Data Communications Protocol Standards Technical Management Panel (DTMP) Working Group 3 on Security. DTMP functional standards are functional groupings of base standards. Referenced base standards may be commercial, DoD, or de facto standards, although International Standards (produced by ISO, CCITT, and other bodies) are preferred when possible.

This part of MIL-STD-2045-18500 contains two normative annexes and two informative annexes.

This document forms part of a DoD Standardized Profile (DSP) for the Message Security Protocol (MSP) covering Message Security requirements, AMHxn(D), for DoD. It is outside of the current Taxonomy and Framework for International Standardized Profiles. It will correspond to the DoD extensions to that taxonomy found in MIL-HDBK-829. This MIL-STD is a content-specific profile for the MSP content type as defined in the Secure Data Network System (SDNS) Specification, SDN.701.

The current technical content of the document has been derived wherever possible from the Secure Data Network System (SDNS) MSP specification SDN.701.

The Preparing Activity for this standard is the Data Communication Protocol Standards Technical Management Panel (DTMP). The custodians for the document are identified in the Defense Standardization Program, "Standardization Directory (SD-1)" and are classified in the Federal Supply Classification (FSC) system under Data Communication Protocol Standards (DCPS). Additional information can be obtained from:

Joint Interoperability and Engineering Organization
ATTN: DTMP Chairman
Building 286
Ft. Monmouth, New Jersey 07703-5613

Contents

Annexes

Figures

Tables

Introduction

This DoD Standardized Profile (DSP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles", and MIL-HDBK-829. The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific, well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and provide a basis for developing uniform, internationally recognized system tests.

One of the most important roles for a DSP is to serve as the basis for the development of recognized tests. DSPs also guide implementors in developing systems that fit the needs of the U.S. Department of Defense (DoD). DSPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other DSPs is crucial to successful realization of this goal.

The specifications in this part of MIL-STD-2045-18500 cover the provision and use of the Message Security Protocol (MSP) to be used with DSP AMH1n(D), Message Handling Systems - Common DoD Messaging. Although this document primarily addresses the use of MSP with X.400 Message Handling Systems, MSP also may be used to encapsulate secure messages in other message environments.

This part of MIL-STD-2045-18500 contains the two normative annexes and two informative annexes listed below.

Annex A Elements of Service (normative)

Annex B Amendments and corrigenda (normative)

Annex C Specific DoD requirements (informative)

Annex D MSP rationale and implementation considerations (informative)

Information technology - Defense Standardized Profiles AMHxn(D) - Message Handling Systems - Message Security Protocol

Part 1 : MSP Service Support

1 Scope

1.1 General

MIL-STD-2045-18500 contains the specifications for supporting Elements of Service and other aspects of the Message Handling portion of Message Handling Systems (MHS), functionality which are specific to the Message Security Protocol (MSP) environment. These specifications are part of the Message Security application functions defined in MIL-STD-2045-18500, and are based on the Common DoD messaging content type-independent specifications in MIL-STD 2045-17501. MSP is content independent and may be used with any DoD MHS protocol.

The specifications in this part of MIL-STD-2045-18500 are divided into basic requirements, which all MHS implementations must support, and several optional functional groups. These optional groups cover significant discrete areas of related functionality that need not be supported by all implementations.

This DoD Standardized Profile (DSP) uses the Common DoD Messaging MIL-STD 2045-17501. It specifies the additional requirements needed to support the content type for MSP.

1.2 Position within the taxonomy

This part of MIL-STD-2045-18500, AMHxn(D) is the first of five parts of a DSP for Message Handling Systems - Message Security. This DSP consists of the following:

Part 1 - Message Security Protocol (MSP) Service Support

Part 2 - AMHx1(D) - MSP Content Protocol

Part 3 - AMHx2(D) - MSP Requirements for Message Transfer (P1)

Part 4 - AMHx3(D) - MSP Requirements for MTS Access (P3)

Part 5 - AMHx4(D) - MSP Requirements for MS Access (P7)

This DSP must be combined with the DSP called “AMH1(D), Message Handling Systems - Common DoD Messaging” (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

The multipart AMH1(D) DSP consists of the following :

Part 1 - MHS Service Support

Part 2 - Specification of ROSE, RTSE, ACSE, Presentation, and Session Protocols for Use by DoD MHS

Part 3 - AMH11(D) - Message Transfer (P1)

Part 4 - AMH12(D) - MTS Access (P3)

Part 5 - AMH13(D) - MS Access (P7)

It may be combined with any DoD approved T-Profile (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

1.3 Scenario

MSP is an end user to end user protocol which defines, for an X.400 message, a new message content, including the security heading and the original content type. MSP is independent of the message content being protected.
Figure 1 depicts the MSP user agent and the functional entities required to provide MSP security services. MSP uses the X.500 Directory to obtain recipient certificates, User Keying Material (UKM), and Auxiliary Vectors (AV). The Key Management System (KMS) is required for rekey operations. The provision of and access to the Message Transfer System (MTS), X.500 Directory and Key Management System is outside the scope of this profile.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of MIL-STD-2045-18500. At the time of publication, the editions indicated were valid. All documents are subject to revision, and

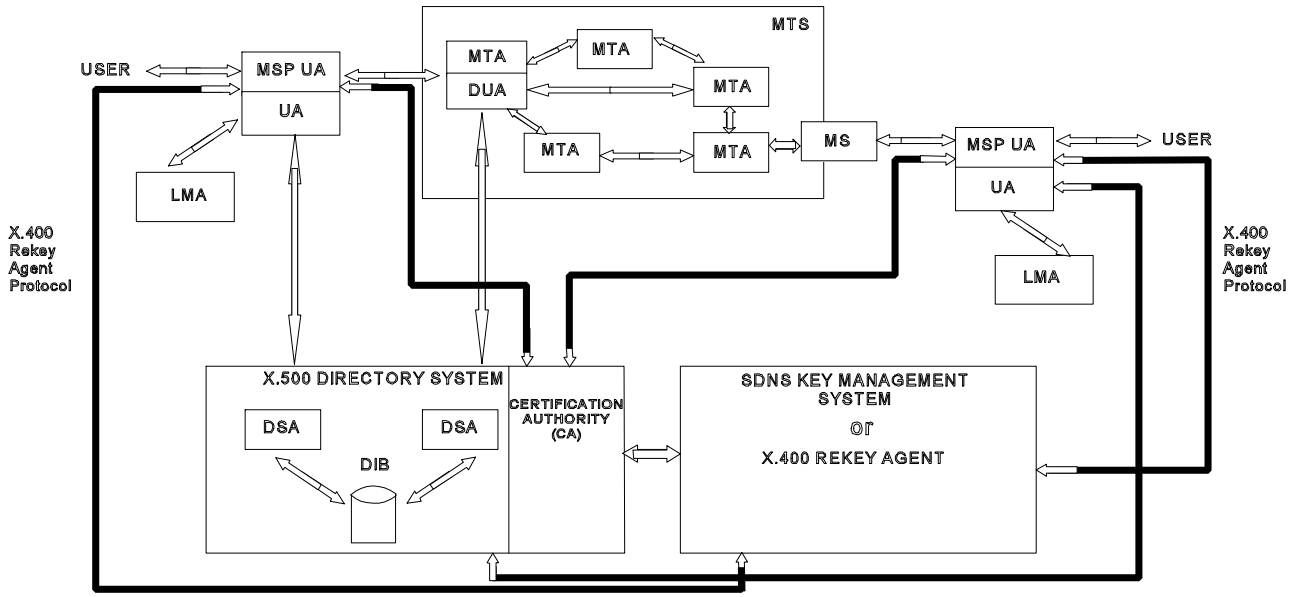

Figure 1 MSP Scenario

parties to agreements based on this part of MIL-STD-2045-18500 are warned against automatically applying more recent editions of the documents listed below, since the references made by DSPs to such documents may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTE -References in this part of MIL-STD-2045-18500 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

Government documents

MIL-STD 2045-17501 Part 1,*Information technology - DoD Standardized Profiles - Message Handling Systems - Common DoD Messaging.*

MIL-HDBK 829, Volumes 1 , *Mil-Std 2045 Series Documentation, 23 April 1993*

MIL-HDBK 829, Volumes 2 , *Guidelines for Data Communications Protocol Standards (DCPS) DoD Standardized Profiles (DSPs), 23 April 1993*

SDN.701: *Message Security Protocol, Revision 2.0, December 11, 1992*.

SDN.702: *SDNS Directory Specifications for Utilization with the SDNS Message Protocol, Revision 2.2, April 29, 1993.*

SDN.703: *SDNS X.400 Rekey Agent Protocol, Version 1.0, November 20, 1991.*

SDN.801: *SDNS Access Control Concept Document, Revision 1.3, July 26, 1989.*

SDN.802: *SDNS Access Control Specification, July 25, 1989*.

DoD activities may obtain copies of DoD directives through their own publication channels or from the DoD Single Stock Point, Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094. Other federal agencies and the public may purchase copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

International Standards Organization (ISO)

ISO 7498-2: 1990, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

ISO 8824: 1990, *Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).*

ISO/IEC 9594: 1990, *Information technology - The Directory. [see also CCITT Recommendations X.5xx(1988)]*

ISO/IEC 9594-8: 1990, *Information technology - The Directory - Part 8: Authentication framework. [see also CCITT Recommendation X.509(1988)]*

ISO/IEC TR 10000-1: 1990, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1990, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-1: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 1: Service Overview. [see also CCITT Recommendation X.400(1988)]*

ISO/IEC 10021-2: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1988)]*

ISO/IEC 10021-4: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 4: Message Transfer System: Abstract Service Definition and Procedures. [see also CCITT Recommendation X.411(1988)]*

ISO/IEC 10021-5: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 5: Message Store: Abstract Service Definition. [see also CCITT Recommendation X.413(1988)]*

ISO/IEC 10021-7: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 7: Interpersonal messaging system. [see also CCITT Recommendation X.420(1988)]*

ISO/IEC Draft pDISP 10611:----[1], *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging*

(Application for copies of these documents should be addressed to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of this part of MIL-STD-2045-18500, this sections contains additional definitions that apply. Terms used in this part of MIL-STD-2045-18500 are defined in the referenced base standards.

3.1 General

Basic requirement An Element of Service (EoS), protocol element, procedural element, or other identifiable feature specified in the base standards that must be supported by all MHS implementations.

Functional group A specification of one or more related EoS, protocol elements, procedural elements, or other identifiable features specified in the base standards that together support a significant optional area of MHS functionality.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at an external interface, i.e., via a communications protocol. Other forms of exposed interface, such as a standardized API, are outside the scope of this version of MIL-STD-2045-18500.

3.2 Support classification

To specify the support level of EoS for this part of MIL-STD-2045-18500, the following terminology is defined.
Mandatory support (m):

for origination:

For Message Transfer (MT) and Message Store (MS) Element of Service (EoS):

A service provider shall be able to make the EoS available to a service user in the role of originator; a service user (a UA) shall be able to use the EoS in the role of originator.

For MSP EoS:

A service provider (a MSP UA) shall implement all procedures specified in the base standards that are associated with providing the EoS, including any corresponding MT or MS EoS. Where specified in the base standards, a service provider shall make the EoS available to a service user in the role of originator. In all cases, the Protocol Implementation Conformance Statement (PICS) shall state whether the EoS is made available to the service user and if so, how.

for reception:

For MT and MS EoS:

A service provider shall be able to make the EoS available to a service user in the role of recipient.

A service user (a UA) shall be able to use the EoS in the role of recipient.

For MSP EoS:

[1] To be published.

A service provider (a MSP UA) shall implement all procedures specified in the base standards that are associated with providing the EoS, including any corresponding MT or MS EoS.

Where specified in the base standards, a service provider shall make the EoS available to a service user in the role of originator. In all cases, the PICS shall state whether the EoS is made available to the service user and if so, how.

Optional support (o) An implementation is not required to support the EoS. If support is claimed, then the EoS shall be treated as if it were specified as mandatory support.

Conditional support (c) The EoS shall be supported under the conditions specified in this part of MIL-STD-2045-18500. If these conditions are met, the EoS shall be treated as if it were specified as mandatory support. If these conditions are not met, the EoS shall be treated as if it were specified as optional support unless otherwise stated.

Out of scope (i) The EoS is outside the scope of this part of MIL-STD-2045-18500. It will not be the subject of a DSP conformance test. However, the handling of associated protocol elements may be specified separately in the subsequent parts of this DSP.

Not applicable (–) The EoS does not apply in the particular context in which this classification is used.

Prohibited (x) The EoS may not be used in an implementation claiming conformance to this profile.

4 Abbreviations

ACSE Association Control service Element
AMH Application Message Handling
ASN.1 Abstract Syntax Notation One
AV Auxiliary Vector
CA Certification Authority
CCITT International Telegraph and Telephone Consultative Committee
DIB Directory Information Base
DoD Department of Defense
DSA Directory Service Agent
DSP DOD Standardized Profile
DUA Directory User Agent
EMS Express Mail Service
EoS Element of Service
FG Functional Group
IEC International Electrotechnical Commission
ISO International Organization for Standardization
ISP International Standardized Profile
KMS Key Management System
LMA Local Management Authority
LRBAC Local Rule-Based Access Control
MHS Message Handling Systems
ML Mail List
MLA Mail List Agent
MOTIS Message-Oriented Text Interchange Systems
MS Message Store
MSP Message Security Protocol
MSP UA Message Security Protocol User Agent
MT Message Transfer
MTA Message Transfer Agent
MTS Message Transfer System
OSI Open Systems Interconnection
PICS Protocol Implementation Conformance Statement
PRBAC Partition Rule-Based Access Control
QoS Quality of Service
ROSE Remote Operation Service Element
RTSE Reliable Transfer Service Element
SDNS Secure Data Network System
UA User Agent
UKM User Keying Material

Support level for EoS (see 3.2):

m mandatory support
o optional support
c conditional support
i out of scope
– not applicable
x prohibited

5 Conformance

No conformance requirements are specified in this part of MIL-STD-2045-18500.

NOTE - This part of MIL-STD-2045-18500 is a reference specification of the basic requirements and functional groups covered by the AMHXn(D) set of profiles and is additional to the protocol-specific requirements specified in parts 2-5 of MIL-STD-2045-18500. Although this part of MIL-STD-2045-18500 contains normative requirements, there is no separate conformance to this part (i.e., it is not identified in the MHS taxonomy) since such requirements are only significant when referenced in the context of a particular protocol.

Parts 2-5 of MIL-STD-2045-18500 specify conformance requirements by protocol for each MHS component with reference to the specifications in this part. Support of the functionality as specified in this part may only be verifiable where the effect of implementation can be determined at a standardized external interface, i.e., via a standard OSI communications protocol. Further, the provision of EoS and other functionality at a service interface will not necessarily be verifiable unless the interface is in the form of a standard OSI communications protocol. Other forms of exposed interface (such as a human user interface or a standardized Application Program Interface (API)) may be provided, but are not required for conformance to this version of MIL-STD-2045-18500.

6 Basic requirements

Annex A specifies additional requirements outside of those specified in Common DoD Messaging MIL-STD 2045-17501 Part 1. The additional requirements include the basic requirements for support of the MSP EoS for conformance to SDN.701. Basic requirements specify the level of support required by all MSP implementations. The MSP UA provides these services by encapsulating the message content and adding the MSP heading before submitting the message to the message transfer system. MSP is transparent to the X.400 MTS.

An MSP User Agent (UA) implementation shall be able to generate an MSP content type. The MSP UA shall offer following security services: Confidentiality, Data Origin Authentication, Connectionless Integrity, and Access Control; Non-repudiation with proof of origin; and Non-repudiation with proof of delivery.

The MSP UA shall be able to determine message security label information either implicitly, based on local processing context, or explicitly, based on a message security label argument.

7 Functional groups

The requirements for functional groups are as specified in clause 7 of the Common DoD Messaging MIL-STD 2045-17501 Part 1.

8 Naming and Addressing

The requirements for Naming and Addressing are as specified in clause 8 of the Common DoD Messaging Mil-Std 2045-17501 Part 1.

Annex A

(normative)

Elements of Service

In the event of a discrepancy becoming apparent in the body of this part of MIL-STD-2045-18500 and the tables in this annex, this annex is to take precedence.

In each table, the "Profile" column reflects the level of support required for conformance to this profile. The "base standard" referred to is those aspects of X.400 required by the content type for the Message Security Protocol as defined in SDN.701.

A.1 MT Elements of Service

There are no additional requirements on MT Elements of Service in this part of MIL-STD-2045-18500.

Table A.1 - Elements of service Belonging to The Basic MT Service (no additional requirements)

Table A.2 - MSP (MT Service) Optional User Facilities

Element of Service	Profile	
	Orig.	Rec.
Additional Physical Rendition	o	–
Alternate Recipient Allowed	m	–
Alternate Recipient Assignment[1]	–	-
Basic Physical Rendition	o	–
Content Confidentiality	o	o
Content Integrity	o	o
Conversion Prohibition	m	-
Conversion Prohibition in Case of Loss of Information	o	-
Counter Collection	o	–
Counter Collection with Advice	o	–
Deferred Delivery	o	–
Deferred Delivery Cancellation	c[2]	–
Delivery Notification	m	–
Delivery via Bureaufax Service	o	–
Designation of Recipient by Directory Name	m	m
Disclosure of Other Recipients	o	m
DL Expansion History Indication	–	m

Element of Service	Profile	
	Orig.	Rec.
DL Expansion Prohibited	m[3]	–
EMS (Express Mail Service)	o	–
Explicit Conversion	o	–
Grade of Delivery Selection	m	m
Hold for Delivery	–	c[4]
Implicit Conversion	–	-
Latest Delivery Designation	m	-
Message Flow Confidentiality	i	i
Message Origin Authentication	o	o
Message Security Labelling	o	o
Message Sequence Integrity	o	o
Multi-destination Delivery	m	–
Non-repudiation of Origin	o	o
Non-repudiation of Submission	i	–
Ordinary Mail	o	–
Originator Requested Alternate Recipient	o	–
Physical Delivery Notification by MHS	o	–
Physical Delivery Notification by PDS	o	–
Physical Forwarding Allowed	o	–
Physical Forwarding Prohibited	m	–
Prevention of Non-delivery Notification	o	–
Probe[5]	ix	–
Probe Origin Authentication	i	–
Proof of Delivery	o	o
Proof of Submission	i	–
Redirection Disallowed by Originator	m	–
Redirection of Incoming Messages	–	o
Registered Mail	o	–
Registered Mail to Addressee in Person	o	–
Report Origin Authentication	i	i
Request for Forwarding Address	o	–
Requested Preferred Delivery Method	o	-
Restricted Delivery	–	i
Return of Content	ix	-
Secure Access Management	m	m

Non-repudiation of Origin	o	o
Non-repudiation of Submission	i	–
Special Delivery	o	-
Undeliverable Mail with Return of Physical Message	o	-
Use of Distribution List	m[6]	-

Notes:

1. The method by which an alternate recipient is specified to support the MTA is outside the scope of this DSP.

2. Messages should be held in the originating MTA to provide support for Deferred Delivery and Deferred Delivery Cancellation. If Deferred Delivery is supported, Deferred Delivery Cancellation must also be supported.

3. Support for this EoS has been made mandatory as the default is DL expansion-allowed.

4. Hold for Delivery in a P3 environment may be determined by local or national policy.

5. Although support for Probes is required for MTAs in the base X.400 standard, support by MTS-users is not required. This profile further makes Probes dynamically prohibited.

6. Use of Distribution Lists on submission is always possible as DLs cannot be distinguished from other O/R addresses.

A.2 MS Elements of Service

A Message Store is optional in the MSP profile, however, if one is implemented, the following Elements of Service apply.

The requirements for support of MS EoS byan MS or UA are as specified in clause A.2 of MIL-STD 2045-17501 Part 1.

Table A.3 - Base Message Store

There are no additional requirements on Base Message Store in this part of MIL-STD-2045-18500.

Table A.4 - MS Optional User Facilities

There are no additional requirements on MS Optional User Facilities in this part of MIL-STD-2045-18500.

A.3 MSP Elements of Service

The following tables specify the requirements for support of MSP Elements of Service by an MTS-user in an MSP environment (i.e. MSP UA) for conformance to MIL-STD-2045-18500.

In the following tables, the "Profile" column reflects the basic requirements for conformance to MIL-STD-2045-18500 -i.e. the minimum level of support required by all MSP implementations conforming to this profile (see clause 6).

Table A.5 - MSP User Facilities

Element of Service	Profile	
	Orig.	Rec.
Access Control	m	m
Content Description	m	m
Connectionless Confidentiality	m	m
Connectionless Integrity	m	m
Forward Signed Message	m	m
Message Origin Authentication	m	m
Non-Repudiation of Delivery[1]	m	m
Non-Repudiation of Origin[1]	m	m
Signed Message	m	m
Traveling User Package	o	m
Mail List[2]	m	m

Note:
1. The names of these EoS are similar to those in X.400, but are MSP specific.
2. Support for this EoS on origination means you can address a Mail List (ML) and support on reception means you can receive a message that has been processed by a ML.

Annex B

(normative)

Amendments and corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and are considered as normative references in this part of MIL-STD-2045-18500.

NOTE - Corresponding corrigenda to the equivalent CCITT Recommendations are contained in the joint CCITT/ISO MHS Implementor's Guide.

MOTIS

ISO/IEC 10021-1/Cor.1:1991

ISO/IEC 10021-1/Cor.2:1991

ISO/IEC 10021-1/Cor.3:1992

ISO/IEC 10021-1/Cor.4:1992

ISO/IEC 10021-1/Cor.5:1992

ISO/IEC 10021-2/Cor.1:1991

ISO/IEC 10021-2/Cor.2:1991

ISO/IEC 10021-2/Cor.3:1992

ISO/IEC 10021-2/Cor.4:1992

ISO/IEC 10021-4/Cor.1:1991

ISO/IEC 10021-4/Cor.2:1991

ISO/IEC 10021-4/Cor.3:1992

ISO/IEC 10021-4/Cor.4:1992

ISO/IEC 10021-4/Cor.5:1992

ISO/IEC 10021-5/Cor.1:1991

ISO/IEC 10021-5/Cor.2:1991

ISO/IEC 10021-5/Cor.3:1992

ISO/IEC 10021-5/Cor.4:1992

ISO/IEC 10021-5/Cor.5:1992

Annex C

(Informative)

Specific DoD Requirements

Quality of Service (QoS), Security, and other unique DoD requirements are addressed with the modifications to ISO/IEC ISP 10611. Listed below are the changes that have been made along with the rationale behind each modification:

C.1 Quality of Service.

As specified in MIL-STD-2045-17501 Part 1 Annex C.

C.2 Security.

1. Use of this profile may preclude the use of other X.400 security services.
2. MSP requires use of the X.500 directory system to obtain the recipient's O/R Address, Certificate, and User Keying Material.
3. As specified in MIL-STD-2045-17501 Part 1, the use of probe EoS is prohibited.

Annex D

(Informative)

MSP - rationale and implementation considerations

D.1 Introduction

The requirement for secure electronic mail and secure messaging resulted in the development of a security protocol to be used with the CCITT X.400 Message Handling System. This protocol is called the Message Security Protocol (MSP).

While the MSP specification is oriented around the X.400 Message Handling System, MSP also may be used as a secure message encapsulation facility with other message environments.

D.2 Concept

MSP provides security services for X.400-based electronic messaging. MSP is an application layer protocol that operates between originator and recipients of messages. As an end-user-to-end-user protocol that does not involve the intermediate message transfer system, MSP provides writer-to-reader security.

MSP encapsulates the original (unprotected) content of an X.400 message, performs security processing, and adds a security heading. MSP defines a new message content type (see figure 2) which is submitted to the X.400 message transfer system.

D.3 General principles

D.3.1 Security services

The security services provided by this MSP include:

- Connectionless Confidentiality, Data Origin Authentication, Connectionless Integrity, and Access Control
- Non-repudiation with proof of origin (message signature)
- Non-repudiation with proof of delivery (signed receipts)

Confidentiality, data origin authentication, and integrity are provided through encryption of the message content and associated key management mechanisms. Access control within MSP involves rule-based access control. Based on the sensitivity and the authorization of the originator, recipient, and workstation, MSP makes the access control decision Identity-based access controls are the responsibility of the originator, supported by the strong authentication provided by MSP. Non-repudiation with proof of origin involves generating a digital signature that allows a recipient to establish the authenticity of a message and the originator's identity to a third party. Non-repudiation with proof of delivery is

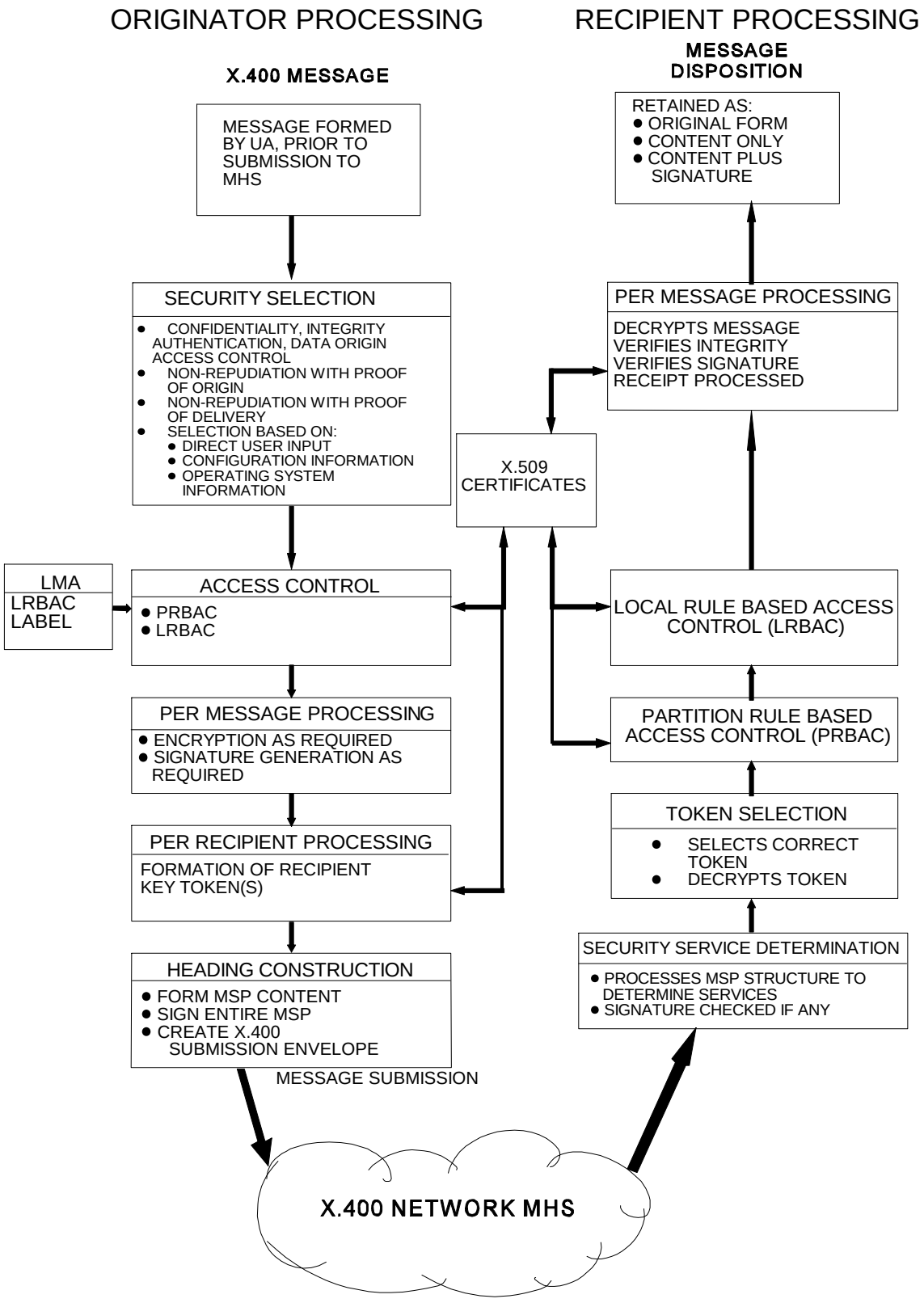

Figure 2 MSP Processing

provided through the return of receipt signed by the recipient and allows the originator to establish to a third party that the message was received by the recipient. This receipt is bound to the original message through the signature; consequently, this service may be requested only for signed messages.

D.3.2 Overview of Protocol

MSP processing consists of originator processing and recipient processing. After originator processing, the message is submitted to the Message Transfer System and is handled just as any other message. Once the message is delivered to the recipient's user agent and the content has been identified as an MSP content, recipient processing begins.

D.3.2.1 Originator processing

MSP processing begins after the message originator has created an X.400 message, and is independent of the content type. This message may be created using any local message preparation system. MSP originator processing consists of the following steps:

1) Security service selection

2) Access control

3) Per-message encryption and signature generation

4) Per-recipient token generation

5) MSP heading construction

6) Message submission

D.3.2.1.1 Security selection

Security selection involves determining which security services are to be performed for the message. The selection information includes the message security label, whether to encrypt and/or sign the message, confirmation of recipients, determination of receipt request information, and provisions for a content description.

D.3.2.1.2 Access control

Access control is the determination of the authorization of the user to send the message and the recipient to receive it.

D.3.2.1.3 Per-message processing

Per-message processing involves the application of security services to the X.400 message content. This entails encryption and signature generation. Integrity is obtained by calculating a hash value over the unprotected message content. If confidentiality is selected, the message content is encrypted with a message key[2]. If non-repudiation with proof of delivery is requested, the originator must request which recipients are to send receipts. If non-repudiation with proof of origin is selected (it must be selected if non-repudiation with proof of delivery is selected), a signature unique to the originator and the unprotected message is generated.

D.3.2.1.4 Per-recipient processing

Per-recipient processing involves the generation of recipient tokens used to pass security information related to confidentiality, integrity, data origin authentication, and access control. These tokens are encrypted with a pairwise key so that only the

[2] How message key is obtained is outside the scope of the MSP specification 2.0.

recipient can decrypt its token. The pairwise key is unique for the message and is created from information obtained from the recipient's X.509 certificates. The X.509 certificates can be stored locally or in a directory system.

D.3.2.1.5 MSP heading construction

MSP heading construction involves the formation of the MSP content or signed Msp content from information obtained above. An unprotected content description may be included with this information depending on local security policy. The entire Msp sequence then may be signed to create a signed Msp content.

D.3.2.1.6 Message Submission

The MSP UA creates an X.400 submission envelope based on the results of the preceding processing, and based on information obtained from the original submission envelope, which accompanied the message content. The MSP AU includes in this submission envelop either Msp or SIGNEDMsp. The MSP UA submits this envelope to the MTS for transfer and delivery.

D.3.2.2 Recipient processing

D.3.2.2.1 Receiving an MSP message

Receiving a secure message begins when the user examines a mailbox (possibly containing both MSP protected and unprotected X.400 messages) and selects a message for processing. MSP recipient processing consists of the following steps:

1) Security service determination

2) Token selection (for encrypted messages)

3) Partition rule-based access control (PRBAC)

4) Local rule-based access control (LRBAC)

5) Per-message processing (decryption, signature validation, receipt generation)

6) Message disposition

First, MSP determines if the MSP structure has been signed. If it has been signed, the signature is verified. MSP then examines the structure to determine what security has been placed on the message. If confidentiality has been selected, the recipient must select the correct token. The recipient decrypts the token with a pairwise key generated from information contained in the X.509 certificates.

D.3.2.2.2 Access control

Access control is a determination of the authorization of the recipient to process and receive the message. These authorizations are based on the authorization information of the originator, the recipient, and the recipient's end system. Two levels of access control are checked, PRBAC and LRBAC. If the PRBAC check passes, the LRBAC information is extracted from the MSP header. An LRBAC check is made, and if that check passes, the message is processed.

D.3.2.2.3 Signature verification

From the recipient's token, the message key is obtained and the message is decrypted. A hash is calculated on the message content and compared to the message hash contained in the header to verify the content's integrity. If the content was signed, the signature is verified. If the originator has requested receipts, then receipt processing is performed. The receipt is a signed hash value, where the hashvalue is calculated over the same data as the originator's hash, followed by some receipt information.

D.3.2.2.4 Message disposition

The final part of the recipient processing is the disposition of the message. An MSP message may be retained in at least three forms: original form (exactly how it arrived prior to any processing), content only (without any MSP header information), or content with signature (content retaining the message signature information to provide non-repudiation and to support forwarding).

D.3.2.2.5 Forwarding

One of the characteristics of the non-repudiation service provided by message signatures is the ability to establish the identity of the originator to a third party. Since the forwarding of messages is a standard part of electronic message systems, MSP includes the ability to forward signed messages. As part of message creation and MSP originator processing, an originator may elect to forward a signed message. This requires that when the message was received, it was saved as either a complete MSP message or as a content plus signature.

D.3.2.3 Travelling users

One of the features that users have come to expect from electronic messaging systems is the ability to access their messages while they are travelling. A common scenario involves the use of a local host to read or send messages. MSP allows users to exchange electronic messages securely, and the Travelling User facility gives users who are away from their home facility a comparable level of access to MSP-protected message services. The principal element of the approach is the ability of the user while travelling to have his cryptographic material available at a remote site.

A travelling user is a user who is visiting an MSP equipped facility other than that which he normally processes messages and who wishes to read or originate MSP messages. This facility allows the travelling user the ability to process MSP secured messages at remote sites with the following features:

1) Ability to perform all MSP message processing functions at a remote site

2) Ability to visit multiple destinations

3) Ability to identify destinations after departure

4) Ability to prepare for remote MSP access in advance so as to have the capability "on tap"

5) Provide accountability consistent with the COMSEC Material Control System

6) Prevent disclosure of, or access to, user cryptographic material at intermediate sites (including COMSEC Custodian devices)

As an additional benefit, this approach supports the local reliability, survivability, and recovery of user keying material. The travelling user package prepared by the user to support local access also can be used to restore the user's capabilities in a local MSP device if the user's MSP device fails.

D.3.2.4 Mail lists

The description of originator processing indicates that MSP generates a token for each recipient of the message. This process can cause a significant performance impact for messages sent to a large number of recipients. Consequently, MSP includes support for Mail List Agents (MLAs). An MLA appears as a normal message recipient and acts as a message expansion point for a Mail List (ML). The administrator of a ML is responsible for establishing rules governing the submission of messages to the list and ensuring that all members of the ML have appropriate access control authorizations. The originator of a message directs the message to the MLA, which then redistributes the message to the members of the ML. This process off loads the per-recipient processing from the individual user agent to and allows for more efficient management of large MLs. Mail lists implementation is out of scope of this MIL-STD.

D.3.2.5 MSP interfaces

MSP may interface with the directory system for management of the required X.509 certificates, User Keying Material, and Auxiliary Vectors (used for LRBAC). Certificates are signed by the Certificate Authority (CA), who vouches for the user and for the binding between the user and the keying material incorporated within the X.509 certificate. The CA is used to authenticate a recipient's certificate and to sign a user's own certificate before being placed in the directory.

D.3.2.6 Rekey operations

For rekey operations, the MSP is required to communicate with the Key Management System. This can be accomplished via the X.400 Rekey Agent Protocol or the SDNS Key Management Protocol. The X.400 Rekey Agent Protocol allows X.400 Rekey Agents to exist outside the perimeter of the SDNS KMS and serve as an intermediary between the two. Certificates are formed from the material obtained from the X.400 Rekey Agent, signed by the CA, and then posted to the directory.

The local management authority(LMA) issues and authenticates (with signature) auxiliary vectors (AVs). MSP uses AVs to make LRBAC decisions.